RESPONSE

This is a response to the Office Action dated February 14, 2006. Claims 1-49 are pending in the application. In the Office Action, the Examiner objected to various informalities in the specification and claims. The specification and claims have been amended to correct these informalities. No new matter has been added with the amendments. The Examiner rejected claims 1 and 49 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 12, 27, 29 (as filed and prosecuted 43, 58 and 60) of U.S. Patent 6,990,395, Application No. 10/689,895. With this response, the Applicants are filing a terminal disclaimer.

The Examiner rejected claims 1, 25 and 49 under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,764,155 ("Kertesz"). Claims 2-14, 16-24, 26-37 and 39-48 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kertesz. "Official notice is taken that network and computer based communications using security measures was well know at the time of the invention was made in analogous art of U.S. Pat. No. 6,263,313 ("Milsted"), U.S. Pat. No. 6,112,304 ("Clawson"), and U.S. Pat. No. 5,862,325 ("Reed")." Office Action of 09/19/05, p. 13, para. 30. Claims 15 and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kertesz, in view of the official notice and further in view of U.S. Pub. No. 2001/0002485 ("Bisbee").

The rejections from the Office Action of February 14, 2006 are discussed below in connection with the various claims. No new matter has been added. Reconsideration of the application is respectfully requested in light of the following remarks.

I.   **SPECIFICATION AND CLAIM OBJECTIONS**

The Examiner objected to the specification as containing an informality. With this response, the paragraph 50 of the specification have been amended to correct the error noted by the Examiner. No new matter has been added. In particular, the following corrections have been made: The "(not shown)" has been deleted following the reference to 211 in paragraph 50. The Examiner objected to the claims as containing various informalities. With this response, claims 19, 20, 26, and 49 have been amended to correct the informalities.

II.   DOUBLE PATENTING

The Examiner rejected claims 1 and 49 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 12, 27, 29 (as filed and prosecuted 43, 58 and 60) of U.S. Patent 6,990,395, Application No. 10/689,895. Additionally, claims 1, 25 and 49 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 126, 127 (as filed and prosecuted 248-250) for claims 1 and 49 and over claims 83, 97 (as filed and prosecuted 212, 243) of U.S. Patent 6,961,641, Application No. 09/723,564. Applicant apologizes to the Examiner for failing to address this rejection with the first Office Action response. With the current response, the Applicants are filing a terminal disclaimer for U.S. Patents 6,990,395 and 6,961,641.

III.   REJECTIONS UNDER 35 U.S.C. § 102

The examiner rejected claims 1, 25 and 49 under 35 U.S.C. § 102(b) as being anticipated by Kertesz. Kertesz discloses "[a] dynamic data exchange (DDE) server which allows external programs to access power management data is presented. The DDE server provides a mnemonic cross reference between register items and standardized, alphanumeric parameter names." Kertesz, Abstract. Kertesz further discloses that "[t]he DDE server acts as a link between a client requesting device data and a field device which can provide the data. The DDE server communicates to the field device through communication ports and to the client via DDE message link." *Id.*

Kertesz fails to disclose an energy management device with a security module as in claims 1 and 49. The security module is "operative to secure said outbound communications and validate said at least one secured inbound communication" according to claims 1 and 49. The DDE Server 152 is shown in Figure 4 and is described as being part of the "computer software used in the power management and control system of the present invention." Kertesz, Brief Desc. of the Drawings. The DDE Server does provide CRC (cyclic redundancy check) check validation. Kertesz, Col. 21, l. 65 – Col. 22, l. 45. However, CRC is a method of detecting errors in transmission. *See e.g.,*

www.computerhope.com/jargon/c/crc.htm. CRC does not provide security in a transmission of data, rather it merely verifies whether the transmission was received correctly. If a CRC error occurs, the receiving unit knows to ask for the transmission to be resent. CRC does not prevent improper third parties from having access to secure information. Specifically, as in amended claims 1 and 25, there is no selective encryption of the communications. The DDE Server does not provide secured communications, although it does provide accurate or reliable transmissions with the CRC error checking.

Accordingly, Kertesz does not disclose secured transmissions. Specifically, according to claims 1 and 25, as amended, there is no disclosure of selectively encrypting outbound communication. Also, there is no disclosure of the validation of secured inbound communications in Kertesz. Even if it was assumed that the energy management device in Kertesz received secured inbound communication (presumably from the Ethernet Gateway), there is no disclosure that the energy management device could validate the secured inbound communication and also selectively encrypt outbound communication. *See* Kertesz, Figure 3. In Kertesz, the energy management device is shown in Figure 3 as number 142. Kertesz does disclose that "[because a] gateway seeks to retransmit packets received from the LAN, it is very important to ensure that these packets did in fact come from the power management system and not other non-related devices (i.e., authentication and security)." Kertesz, Col. 6, ll. 10-14; Col. 47, ll. 4-7. The transfer protocol employed in Kertesz has "a header which contains information regarding the number of bytes in the serial data packet and a checksum byte that ensures that the header itself has not been corrupted." Kertesz, Col. 6, ll. 15-18. "[P]ackets transmitted to the gateway 150 by computer 142 comprise the serial communications data packet plus a fifteen byte header inserted in front of it." Kertesz, Col. 47, ll. 12-15. The security and authentication that occur in Kertesz are located within the Ethernet Gateway 150, and do not occur within the energy management device 142. Therefore, the energy management device 142 does not disclose a security module.

For at least these reasons, Kertesz does not anticipate independent claims 1, 25 and 49, as amended. Accordingly, Applicant requests that the Examiner withdraw this rejection of claims 1, 25 and 49.

IV.   REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 2-14, 16-24, 26-37 and 39-48 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kertesz. Official notice was taken that network and computer based communications using security measures was well known at the time of the invention was made in analogous art of Milsted, Clawson, and Reed. Claims 15 and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kertesz, in view of the official notice and further in view of Bisbee.

Milsted, Clawson, Reed and Bisbee all fail to disclose the elements of independent claims 1 and 25. In particular, these references fail to disclose the security module and secured communications of the claims. In addition, there is no disclosure of secured outbound communications or the validation of secured inbound communications, an energy management function to generate second energy management data, or an energy distribution system interface according the energy management device disclosed in claims 1 and 25. Applicant's acknowledge the Examiner's Official Notice, but respectfully disagrees and points out that the specific security measures in claim 1 and 25 are not known as used by an energy management device in an energy management architecture for managing an energy distribution system. In addition, there is no disclosure of selective encryption for outbound communications according to amended independent claims 1 and 25.
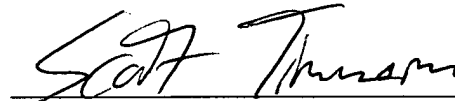
Dependent claims 2-24 and 26-48 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Kertesz. Dependent claims 2-24 and 26-48 should be allowed for the reasons set out above for the independent claims from which they depend. Applicant therefore requests that the Examiner withdraw these rejections of dependent claims 2-24 and 26-48.

V.   CONCLUSION

Each of the rejections in the Office Action dated February 14, 2006 has been addressed and no new matter has been added. Applicants submit that all of the pending claims are in condition for allowance and notice to this effect is respectfully requested. The Examiner is invited to call the undersigned if it would expedite the prosecution of this application.

Respectfully submitted,

Date: <u>May 10, 2006</u>

Scott A. Timmerman
Registration No. 55,678
Attorney for Applicants

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200